Privacy and Security Solutions for Interoperable Health Information Exchange

Report to NCVHS ad hoc committee on secondary health data

Steve Posnack, ONC

Linda Dimitropoulos, RTI

July 17, 2007

Overview and Background

- Brief summary of the contract
- Where we are today
- Where we are going

Assumptions Underlying the Methodology

- Decisions about protecting the privacy and security of health information should be made at the local community level
- Discussions need to take place to develop an understanding of the current landscape and the variation that exists between organizations within each state, and ultimately across states
- Stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the challenges and developing solutions to achieve broad-based acceptance

Overview of the Process

- Community-based research model where states “own” the issues and outcomes
- Engage broad range of stakeholders to identify challenges and develop solutions
- State project teams follow a “core” methodology that frames discussions in terms of purposes for the exchange of certain types of health information within 9 domains of privacy and security

Nine Domains of Privacy and Security

- User and entity authentication
- Authorization and access controls
- Patient and provider identification
- Information transmission security and exchange protocols
- Protection against improper modification
- Information audits
- Administrative or physical security
- State law restrictions
- Information use and disclosure policies

18 Exchange Scenarios

- Treatment
- Payment
- RHIO
- Research
- Law Enforcement
- Prescription Drug Use/Benefit
- Healthcare Operations/Marketing
- Bioterrorism
- Public Health
- Employee Health State Government Oversight

Scenarios Focused on Secondary Data

- RHIO scenario: Request to participating entities to provide identifiable data to monitor incidence and management of diabetic patients
- State Discussion:
  - De-identified data okay to submit to HIE
  - Identifiable data would require IRB approval
  - Uncertain about HIE status under the HIPAA Privacy Rule

Scenarios Focused on Secondary Data (continued)

- Research Data Use and State Government Oversight Scenarios
  - no issues with the use of data for research purposes or oversight if protocols are reviewed by appropriate IRBs and informed consent is obtained from patients if identifiable data are used.

Scenarios Focused on Secondary Data (continued)

- Law Enforcement
  - Stakeholders unclear on the law related to disclosure of health information to law enforcement
  - Hospitals typically require subpoena but there is variation-some release on verbal request
  - Agreement that organizations would not release info to parents because patient over 18 even though on parents insurance
  - Discussion noted that EOB would likely inform parents

Scenarios Focused on Secondary Data (continued)

- Health Care Operations/Marketing
  - 8 states generated a lot of discussion of ethics of using health data for marketing purposes
  - De-identified data for quality improvement was okay
  - Identifiable data would always require authorization
  - 3 states teams said that they would never sell data for 3rd party marketing

For more information

- **http://healthit.ahrq.gov**
- **http://healthit.ahrq.gov/privacyandsecurity**
- **www.rti.org/hispc**

- steven.posnack@hhs.gov
- jonathan.white@ahrq.hhs.gov
- lld@rti.org